North, Central and South Manchester Clinical Commissioning Groups

NHS

Information Governance

IG2 - Information Governance Policy

Version: **2.0**

Date Approved:

Document Control Sheet

Title of document:	IG2 – Information Governance Policy		
Supersedes:	IG1 Information Governance Policy, IG3 Confidentiality and Data Protection Policy IG6 Information Security Policy IG7 Email Policy IG18 Encryption Policy IG12 Information Security Spot Checks		
Placement in Organisation:	Information Governance		
Consultation/Stakeholders	North, Central and South Manchester CCGs		
Author(s) name:	Shavarnah Purves – Senior Information Governance Officer Graham Hayler – Head of BI & IG		
Department /Team:	IG Team		
Approved by:	North Manchester CCG Corporate Governance Committee Central Manchester CCG Corporate Governance Committee South Manchester CCG Corporate Governance Committee		
Approval date:		Review date:	February 2018
Implementation Date:	February 2016		
Implementation Method:	Team briefings/meetings CCG Website		
This document is to be read in conjunction with the following documents: *Records Management Policy* *Acceptable Use Policy*			

Version Control

Version	Date	Brief description of change
V0.1	June 2013	*Amendments to reflect CSU management of CCG Information Governance*
V0.2	August 2013	*Amendments from the Corporate Governance Committee*
V1.0	October 2013	*Corporate Services Team – Information Governance Policies and Procedures Development and Implementation sign off*
V1.1	February 2014	*CSU IG Team reviewed all policies to look at merging some together. These amendments reflect this.*
V2.0	February 2016	*Changes to reflect new IG structure*
V2.1	May 2016	*Changes to reflect new IG Lead*

PLEASE NOTE: the formally approved copy of this document is held on North, Central and South CCG's website. Printed copies or electronic saved copies must be checked to ensure they match the current online version.

Contents

Appendices

1.0	**Policy Statement**
1.1	North, Central and South Manchester Clinical Commissioning Group (hereafter referred to as the CCG or organisation) organisational 'constitution' is a nationally approved document, which outlines the fundamental principles that govern how a CCG functions as stipulated by *'The National Health Service under the Health and Social Care Act (2012)'.*
1.2	These rules, collectively, make up (*i.e. constitute*) what the CCG is required to do. Therefore, when these principles are written into a single document, that document is said to embody a 'written' constitution and henceforth is a recognised legal code by which the CCG will be held accountable
1.3	By virtue of its constitution, the CCG has developed a set of documented principles, to which it is legally accountable to, and therefore, each principal requires a specific set of rules and procedures to guide its decisions and ensure documented evidence of the outcomes is maintained.
2.0	**Introduction**
2.1	This Policy sets out the Information Governance approach in the three Manchester Clinical Commissioning Groups for ensuring that personal information is dealt with: • Confidentiality – Protecting the personal information from unauthorised access, disclosure or processing; • Integrity – Safeguarding the accuracy and completeness of information and systems; • Availability – Ensuring information is available to users when required; • Quality – Ensuring information is fit for the intended purpose.
2.2	Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service.
2.3	Information Governance sits alongside Clinical Governance, Research Governance and Corporate Governance. It provides a framework to bring together all of the requirements, standards and best practice that apply to the handling of personal information. It also provides a consistent way for employees to deal with the many different information handling requirements.
2.4	This document sets out minimum policy standards and common policy directions across the three Manchester Clinical Commissioning Groups (henceforth referred to as "the CCG") for confidentiality, integrity and availability of information (Information Governance). The policy is intended to cover the overlapping areas of: • Confidentiality (with regard to 'common law'); • Data Protection Act 1998 compliance; • Freedom of Information Act 2000 compliance; • Information Security;
2.5	The aims of this document are to ensure that information is: • held securely and confidentially; • obtained fairly and lawfully; • recorded accurately and reliably;

	• used effectively and ethically; • shared and disclosed appropriately and lawfully.
3.0	**Purpose**
3.1	This policy applies to those members of staff directly employed by the CCGs and for whom the CCGs have legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisations' policies are also applicable whilst undertaking duties for or on behalf of the CCGs. This policy applies to all third parties and others authorised to undertake work on behalf of any of the CCGs.
3.2	This policy applies to all forms of information, including but not limited to: • paper and electronic filing systems; • communications, including those sent by post, electronic mail and text messaging; • information that is stored in and/or processed by information systems including servers, personal computers (PCs), any other mobile device; • information that is stored, copied, moved or transferred to any type of removable or portable transmission, both internally or externally to a third party.
4.0	**Responsibilities**
4.1	Overall accountability for procedural documents across the organisation lies with the Accountable Officer who has overall responsibility for establishing and maintaining an effective document management system, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.
4.2	Responsibilities will be given to: • The Caldicott Guardian who will: o ensure that their CCG satisfies the highest practical standards for handling patient identifiable information; o act as the conscience of their CCG; o facilitate and enable information sharing and advise on options for lawful and ethical processing of information; o represent and champion IG requirements and issues at Board level; o ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff; and o oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS. • A Senior Information Risk owner (SIRO) will: o be an Executive Board Member; o take overall ownership of the information aspects within the Risk Policy acting as champion for information risk on the Board and provide advice to the Accountable Officer on the content of their CCG's Statement of Internal Control in regard to information risk; o understand the strategic business goals of their CCG and how other NHS organisations' business goals may be impacted by information risks, and how those risks may be managed; o work with the IG Team to manage the IG risk assessment and management processes within their CCG; o advise their Board on the effectiveness of information risk

management across their CCG;
- receive training as necessary to ensure they remain effective in their role as SIRO.

- Information Asset Owners (IAO) will:
  - lead and foster a culture that values, protects and uses information for the success of their CCG and benefit of its customers;
  - know what is in the asset and what is linked to it. Have an understanding of how the data flows to and from the asset, know who has access to the asset, whether system or information, and why, and ensure access is monitored and compliant with policy;
  - understand and address risks to the asset, providing assurance to their SIRO.

- Information Governance & IT Lead will:
  - manage the Senior Information Governance Officers to deliver Information Governance for the CCGs;
  - ensure the CCG complies with all legislation and NHS Policy in relation to Data Protection, Freedom of Information, Records Management, Caldicott, Confidentiality and Information Security.
  - understand and address risks to the information assets, providing assurance to their SIRO;

- The Senior Information Governance Officers will:
  - supply advice and guidance to all staff on all elements of Information Governance;
  - maintain an awareness of Information Governance issues within the CCGs;
  - review and update the Information Governance Policy in line with local and national requirements providing template documents to the CCGs;
  - ensure line managers are aware of the requirements of the Information Governance Policy;
  - support the SIRO and Caldicott Guardian;
  - support and monitor the Information Governance training requirements for all CCG staff.

- Line managers will take responsibility for ensuring that the IG Policy is implemented within their group or directorate.

- It is the responsibility of each employee to adhere to the policy.

- Staff will receive instruction and direction regarding the policy from a number of sources:
  - policy/strategy and procedure manuals;
  - line manager;
  - specific training course;
  - other communication methods, for example, team meetings; and
  - staff Intranet.

5.0 **IG Framework**

5.1 The IG Framework will be supported by the Information Governance Policy and other related policies and procedures to cover all aspects of IG, which are aligned with the NHS Operating Framework and the IG Toolkit requirements:

- Records Management Policy

	• Information Risk • Secure Transfers of Information Procedure • PIA Proforma Procedure • IG Incident Report Procedure (Appendix of the Incident Reporting Policy. • Subject Access Procedure In addition, the following policies will be part of the IG suite of policies which will be supported by those framework documents, above.
5.2	The Policy framework will encompass the following: • Acceptable Use Policy • Records Management Policy • Secure Transfer of Information Procedure
5.3	An IG Staff Handbook will be issued to all staff this provides a brief introduction to IG and summarises the key user requirements that support the IG policies. This will be available on the staff intranet IG Page.
6.0	**Principles: Confidentiality and Data Protection**
6.1	The CCGs are committed to the delivery of a first class confidential service. This means ensuring that all personal service user and staff information is processed fairly, lawfully and as transparently as possible so that the public can: • understand the reasons for processing personal information; • give their consent for the disclosure and use of their personal information where necessary; • gain trust in the way the CCG handles information; • understand their rights to access information held about them.
6.2	**The Duty of Confidence** All NHS bodies and those carrying out functions on behalf of the NHS have a duty of confidence to service users and a duty to support professional ethical standards of confidentiality. Everyone working for the NHS that handles, stores or otherwise comes across information that is capable of identifying individual service users has a personal duty of confidence to the service user and to his/her employer. The duty of confidence is conferred by common law, statute, contract of employment, disciplinary codes and policies and professional registration. Service users expect that information given by them to their doctors, nurses and other members of the healthcare team is treated in confidence and not passed to others without their permission. Similar considerations apply to personal information concerning other individuals, such as staff. Particular care must be taken to avoid inadvertent or accidental disclosure. The underlying principle is that all information that can be related to an individual must be treated as confidential and it must not be communicated to anyone who is unauthorised to receive it. Unauthorised staff include those who are not involved in either the clinical care of the service user or the associated administration processes. No personal information, given or received in confidence, may be passed to anyone

	else without the consent of the provider of the information. This is usually the service user but sometimes another person may be the source (e.g. relative or carer). No personal information, given or received in confidence for one purpose, may be used for a different purpose without the consent of the provider of the information. Service users are entitled to object to the use of their personal health data for purposes other than their immediate care. The duty of confidentiality owed to a deceased service user must be viewed as being consistent with the rights of living individuals.
6.3	**What is Personal Information?** Personal identifiable information or personal data is strictly defined in the Data Protection Act 1998 to which all organisations processing personal information and all staff within those organisations, must adhere. Personal Information is now commonly known as Personal Confidential Data (PCD). PCD is data in which individuals are clearly identified, or there is a high risk of individuals being identified. This includes patient identifiable data, such as: • NHS number • Name • Address • Postcode • Date of Birth • Date of Death PCD also includes sensitive data which may include items such as: • Racial or ethnic origin • Political opinions • Criminal record • Physical or mental health condition • Religious or other similar beliefs • Sexual life Information that falls into any of the categories above must be regarded as confidential, and must not be used unless absolutely necessary and where there is a legal basis to do so. If an individual is unclear if information should be classified as PCD, they must discuss the issue with their line manager or the IG Team, who will offer advice.
6.4	**Disclosing Information** The CCG IG Staff User Handbook provides advice on using and disclosing confidential service user information and has models for confidentiality decisions. All staff must adhere to this guidance. Personal information may be disclosed on the basis of informed consent where the disclosure is necessary for healthcare purposes and is undertaken by a health professional or a person owing an equivalent duty of confidentiality. Consent of the individual will be required where a disclosure of personal information

	is not directly concerned with the healthcare/treatment of a service user e.g. medical research, health service management, financial audit, personnel data or where disclosure is to a non-health care professional. Under common law, personal information may be disclosed without consent for example: • in order to prevent abuse or serious harm to others; • where the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the service user concerned and the broader public interest in the provision of a confidential service. All individuals must: • exercise all due care and diligence to prevent unauthorised disclosure of confidential information; • ensure the physical security of all confidential documents, including storage of files on PCs. In most circumstances, police should only be given access to personal records with the patients' consent or a court order. Please speak to the Information Governance Team for guidance on the process. Information should only be released to the police after first consulting your line manager and the Caldicott Guardian. Any individual has the right to request to see the information an organisation holds about them. This is called a Subject Access request. Any individual making such a request must do so in writing. The CCG has a Subject Access Procedure in place which all staff must familiarise themselves with and adhere to. Staff should never give information to a person claiming to be the friend, relative or representative of a member of staff/patient/service user. Unless appropriate checks have taken place to ensure that person has a legitimate reason for access. Action of this kind may be viewed as a breach of confidentiality and may lead to an investigation; this may result in disciplinary action being taken.
6.5	**Personnel Information** In keeping with good Human Resources practice, the CCG retains and processes personal data on its employees. In addition, the CCG may from time to time, retain and process "sensitive personal data" as defined by the Data Protection Act 1998 (DPA) for example, in relation to sickness and occupational health records, performance reviews, equal opportunities monitoring and for the prevention of fraud or other illegal activities. The CCG may process such data and such data may be legitimately disclosed to appropriate employees and to CCG professional advisors, in accordance with the principles of the DPA. The CCG takes all reasonable steps to ensure that the data it holds is accurate, complete, current and relevant. If a member of staff considers that data held on him/her may be inaccurate, or if he/she wishes to have access to such data, then contact should be made with the HR Lead.
7.0	**Principles: Information Security**
7.1	The information held and managed by the CCG is an asset that all staff have a duty

	and responsibility to protect. The availability of complete and accurate information is essential to the CCG functioning in an efficient manner. The following information has been taken from the existing IT policies (Information Security, Email & Encryption) for more detailed information on anything below please refer to these policies which can be found on the staff intranet page.
7.2	**Information Security – Requirements** The CCG will implement technical and operational standards, policies and processes that align with prevailing standards such as ISO27001 (Information Security Management). The requirements of policy, processes and procedures will be incorporated into the CCG operational procedures and contractual agreements. Information stored and processed by the CCG will be appropriate to business requirements and no information will be stored or processed unnecessarily. The CCG will develop, implement, maintain and test where required, local business continuity plans. Such plans will be a contractual obligation of any relevant supplier. The CCG will ensure that appropriate controls are applied to all types of communication, internal and external, to ensure the communication is secure, appropriate and reaches the intended recipient. The CCG will undertake risk assessments to identify, quantify and prioritise information security risks in accordance with the Risk Assessment Policy. Controls will be selected and implemented to mitigate the risks identified. All breaches of information security, actual or suspected will be reported and suitably investigated in line with information incident management procedures which will provide guidance on what constitutes an information incident.
7.3	**Asset Management** All CCG information (electronic and hardcopy), software, computer and communication equipment, will be accounted for and have an owner. The CCG will implement controls that will ensure its assets are appropriately protected. Owners of such assets will be responsible for the maintenance and protection of assets they are assigned.
7.4	**Information Systems Acquisition, Development and Maintenance** Information security requirements will be defined and communicated during the development of business requirements for new systems or changes to existing systems. Controls to mitigate risks identified during design, procurement, development, testing and deployment will be implemented.

7.5	**User Access Controls** Only authorised CCG staff or authorised support personnel are permitted to access CCG computers and the information that is held on them. All CCG Staff must have their own unique computer account and only login to systems or applications that they have been granted access to. Access controls must take account of security requirements of the business application and permit access to be granted only on approval by the system administrator in consultation with the appropriate senior manager where there is any concern or doubt. Remote access to the CCG network is protected by strong authentication and passwords. Employees will normally be granted access only to such information that is required to perform their work duties. If they are erroneously granted any other access, then this fact must be reported to their line manager immediately as it may become construed as unauthorised access. Where information is copied between systems within the network, then employees should ensure that any confidential information remains secure and that the recipient system has the same or greater standard of security protection as the sender.
7.6	**Passwords** Only the person to whom a password is issued should use that password and it must not be divulged to anyone else. Any doubts or exceptional circumstances that require disclosure must be referred to the Information Governance Team immediately. If you suspect that your password is known by another user you must change it as soon as possible. If a Systems Administrator is required to do this then it is up to the staff concerned to contact them. Passwords used within the CCG's systems must be a minimum of 6 characters. All staff must change their password when prompted.
7.7	**Encryption** Encryption is the process of converting information using an algorithm to make the information unreadable to anyone except those who have the decryption key. The CCG will ensure all of its electronically held data is adequately protected from loss and inappropriate access. To reduce the risk of unauthorised access the CCG will ensure that the following devices are encrypted by default: • Laptops • Open access Desktops • Handheld devices (where windows OS is used) • Portable storage devices (Memory sticks etc) • Removable media e.g. DVDs and CDs.

	Staff must not bypass, cause to bypass or use tools or software to bypass the encryption software installed on devices. The CCG is also working with clinical system providers to ensure that all GP clinical systems backup tape media are encrypted to the required level. Guidance from the Department of Health and Health & Social Care Information Centre (HSCIC) specifies standards for encryption and a national procurement has taken place to provide the products to achieve these standards. The CCG will ensure that all data stored on the above devices will be encrypted to a minimum of 256bit encryption. The software, processes and procedures to allow this are being implemented throughout the CGG via GM Shared Service IT Department.
7.8	**Anti-Virus** Software and information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses, Trojans and worms. Virus threats are a day to day threat, however the type, strain, and the number of incidents may well increase due to the increase in web activity. This can cause serious disruption to both the user and IT Services. • All CCG computers must run anti-virus software which is constantly updated; • CCG Staff must contact the GM Shared Service IT Service Desk if a virus incident is known or suspected.
8.0	**IG and Records Management**
8.1	The Joint Governance Committee will monitor the implementation and on-going management of the IG Framework and IG Toolkit requirements. The Joint Governance Committee will be responsible for ensuring that the Records Management Policy is implemented and that the records management system and processes are developed, co-ordinated and monitored. The Records Management Policy can be found on the staff intranet.
9.0	**IG Training**
9.1	All staff (including temporary or contractors) are mandated to undertake the Information Governance e-learning module via Central Manchester University Hospitals Foundation Trust (CMFT) E-Learning system on an annual basis. Where relevant further training and education will be required of staff. Staff will be informed by the Training Needs Analysis.
10.0	**Process for Approval & Ratification**
10.1	The process for approval and ratification detailed in the 'Corporate Document Template and Users Guidelines Policy' will be used.
10.2	The Joint Governance Committee is the committee with delegated authority for the approval and ratification of this document. This will be reviewed every 2 years.
11.0	**Dissemination, Training & Advice**
11.1	Staff will receive instruction and direction regarding the policy from a number of

	sources: • policy/strategy and procedure manuals; • line manager; • specific training course; • other communication methods (e.g. team brief/team meetings); • staff intranet.
11.2	This policy and a set of procedural document manuals are available on the staff Intranet.
11.3	Staff will be made aware of procedural document updates as they occur via team briefs, team meetings and notifications via the staff intranet.
12.0	**Review, Monitoring and Compliance**
12.1	This policy will be monitored through staff awareness and supporting evidence within the IG Toolkit.
12.2	This policy will be reviewed regularly, and in accordance with the following on an as and when required basis: • legislative changes; • good practice guidance; • case law; • significant incidents reported; • new vulnerabilities; • changes to organisational infrastructure.
12.3	**Equality impact assessment** The CCGs aim to design and implement services, policies and measures that are fair and equitable. As part of its development, this policy and its impact on staff, patients and the public have been reviewed in line with the CCGs' Legal Equality Duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, patients and the public on the grounds of race, socially excluded groups, gender, disability, age, sexual orientation or religion/belief. Where relevant further training and education will be required of staff. Staff will be informed of this need when the situation arises. The Equality Impact Assessment has been completed and has identified impact or potential impact as "no impact".
13.0	**References**
13.1	• Data Protection Act 1998 • The Common Law Duty of Confidentiality • Confidentiality: NHS Code of Practice (Department of Health) • Health and Social Care (Safety and Quality) Act 2015 • Caldicott Report 2013 • The Public Interest Disclosure Act 1998 • Human Rights Act 2000 • Regulation of Investigatory Powers Act 2000 • Computer Misuse Act 1990

	• Public Records Act 1958
13.2	A set of procedural documents will be made available via the Intranet: • Subject Access Procedure • Registration Authority (Smart Card) Procedure • Information Governance Staff Handbook • Secure Transfer of Information Procedures • Training Need Analysis • PIA Procedures • Information Governance Procedures for 3rd Parties • Confidentiality Audit Procedures This list is not exhaustive.

Appendix A – Section 251 Exemption

When CCGs were introduced they were not given the same legal powers to process PCD as Primary Care Trusts were. The Health and Social Care Act (HSCA) 2012 states that only the Health and Social Care Information Centre (HSCIC) can receive and process PCD, for secondary use without patient consent.

The North West Data Service for Commissioners Regional Office (DSCRO) currently acts as a regional office for the HSCIC and are able to process PCD legally.

Accredited Safe Haven and Controlled Environment for Finance

In light of the information sharing difficulties encountered by CCGs as a result of the HSCA 2012 the Secretary of State introduced 2 exemptions to the Act known as Section 251 to support commissioning activities. These are:-

- **Accredited Safe Haven (ASH)**

  An ASH is an accredited organisation, or a designated part of an organisation, which is contractually and legally bound to process data for commissioning purposes in ways that prevent the identity of individuals. An organisation with ASH status can receive a dataset containing a single patient identifier but the dataset has to be sent via the local office of the Data Service for Commissioners Regional Office (DSCRO) which is based at St James House in Salford.

  Under the terms of the ASH agreement the following data items are classed as patient identifiers and as such an ASH can receive a dataset containing one of these items:
  - Name
  - NHS Number
  - Date of Birth
  - Postcode

  The 3 Manchester CCGs have secured ASH status

- **Controlled Environment for Finance (CEfF)**

  CCGs can become a Controlled Environment for Finance (CEfF) which allows trained staff to process patient identifiable data for invoice validation purposes subject to certain conditions being met.

  In summary patient identifiable data must not be included on the invoice and should be sent separately to secure email addresses only accessible to the nominated and appropriately trained CEfF staff.

Appendix B - Key Contacts

IG Team – Names and Roles

Mark Wright
Information Governance and IT Lead
Mark.wright7@nhs.net

Shavarnah Purves
Senior Information Governance Officer
Supporting SMCCG and Shared/Citywide Services
Shavarnah.purves@nhs.net

Aliyah Ashraf
Senior Information Governance Officer
Supporting NMCCG and CMCCG
aliyah.ashraf@nhs.net

SIRO
NMCCG – Martin Whiting
CMCCG – Ed Dyson
SMCCG – Claudette Elliot

Caldicott Guardian
NMCCG – Dr Mobeen Shahbaz
CMCCG – Dr Manisha Kumar
SMCCG – Dr David Adams-Strump

Appendix D – Information Governance Training Needs Analysis (2016-17)

Information is an extremely valuable resource and is essential for the delivery of high quality services. Good Information Governance (IG) practices ensure necessary safeguards for the appropriate use of business and Personal Confidential Data (PCD) are in place and managed effectively. These safeguards can be found in the policies and procedures applicable to all staff but of equal importance is the knowledge and awareness each individual maintains of IG to recognise and work within these safeguards.

Therefore it is a mandatory requirement that all staff including permanent, temporary, contractors and agency staff will receive appropriate basic Information Governance Training and to have that training refreshed annually.

While there is already an existing requirement within the IG toolkit to annually complete IG training. The importance of this training was also clearly recognised in with recent Caldicott Review 2 which states:

> 'All staff should receive annual basic Information Governance Training appropriate to their role'

The IG training requirement also requires that:

- Basic IG training is provided for all new starters as part of their induction; and
- Additional training is provided to staff in key roles

Basic Mandatory Training

The Manchester CCG's currently use Central Manchester University Hospitals Foundation Trust (CMFT) E-Learning system.

The training can be accessed via the following link http://www.elearning.cmft.nhs.uk/course/view.php?id=282. Your username is your payroll number (ESR number). If you are logging into the e-learning portal for the first time your password will be the default password which is learning. Please note you will be required to change this once you have logged in.

Additional Training

There are key roles within the organisation for example, Senior Information Risk Officer (SIRO), Information Asset Owner (IAO) as well as specific areas that may handle PCD or other types of key information. These key roles or areas will be required to undertake additional IG training relevant to their role. This additional training is necessary to ensure relevant safeguards are full respected.

Principally, additional training will be delivered via the National IG Training Tool as this site has available many more modules covering a range of topics and at various levels. The website can be found using the following link: https://www.igte-learning.connectingforhealth.nhs.uk/igte/index.cfm.

Please note that while you may complete any module that is available you will be required to complete all modules applicable to you as per the IG Training Needs Analysis (TNA):

- Confidentiality and Caldicott
- Information Governance and Information Governance Management
- Information Risk Management
- Information Security

- Records Management
- Refresher Module

You will be informed directly via your line manager or from the IG Team which modules are relevant to your role which you are mandated to complete.

Subject to discussion with the Information Governance Team, additional bespoke sessions can be arranged as required or may be arranged in response to demand.

Departmental Training

To complement the knowledge gained from the e-learning modules and IG range of policies, IG can deliver face to face sessions with each department on an annual basis to support a specific business requirement, including:

- Understanding and application of IG policies and procedures;
- Provision of specific departmental advice and guidance;
- Facilitation of an informal Q&A session.

What training do I have to do?

The IG Training Need Analysis (TNA) matrix highlights the training modules all staff are mandated to complete for Information Governance. It also highlights the additional modules staff having specialist roles must complete.

New Starters/Returning to Work

New starters **to the NHS** must complete their IG Training via the NHS national online training tool using the following link: https://www.igtt.hscic.gov.uk/igte/index.cfm?communityid=2.

If you are a new starter and are already employed within the NHS whether you are permanent, temporary, contractor or agency, you must complete your training within the first 4 weeks of commencing in post using CMFTs E-Learning System. If you have changed roles within the organisation and your new role or area is one of those listed in the TNA then you will be regarded as a new starter in that role.

If you have been absent from work and your required IG training status elapsed during your absence, for example maternity leave, external secondment, career break, or long term sick. You are required to complete your IG training within the first 4 weeks of your return.

Work Experience staff

You are still required to complete an IG assessment. Speak to the Senior IG Officer on how best to complete this. The appropriate modules should be completed within the first four weeks of commencing your placement.

Monitoring and Compliance

Organisations are expected to achieve 95% compliance with Information Governance Training (mandatory module). Compliance against the IG training plan and TNA will be monitored throughout the year with regular reports provided to managers for staff management and governance purposes. All compliance reports published also form the evidence base for external audits.

Information Governance Training Needs Analysis Matrix

All members of staff including permanent, temporary, contractors, agency staff and work placements must complete the mandatory training modules detailed below and in accordance with the following:

- New starters/returning to work, are required to complete within the first 4 weeks of starting or returning to work,
- Staff having completed their introduction or beginner's guide modules only need to complete the 'Refresher module' in every 3 years,
- All other TNA modules are to be completed annually unless otherwise informed,
- All staff must maintain a valid 12 month basic mandatory training pass.

The following table shows the on-line training modules available by Job Role identified within the IG Training Tool and specifies which modules are mandatory and those that are recommended. Please refer to the Key set out at the foot of the table.

JOB ROLE	Modules											
	Information Governance: The Refresher Module	The Caldicott Guardian in the NHS and social care	Introduction to Information Governance	Information Governance: the Beginner's Guide	NHS Information Risk Management: Introductory	NHS Information Risk Management: Foundation	NHS Information Risk Management for SIROs & IAOs	Information Security Guidelines	Secure Transfers of Personal Data	Information Security Management	Records Management in the NHS	Secure Handling of Confidential Info
Admin & Clerical - Access to confidential Information												
Admin & Clerical - No Access to confidential Info												
Caldicott Guardian												
Clinical Staff												
Information Asset Administrator (IAA)												
Information Asset Owner (IAO)												
IG Manager Lead												
IT Management												
Senior Information Risk Owner (SIRO)												

	Mandatory - This module needs to be completed every 3 years once you have passed either Introduction to IG or IG: The Beginner's Guide.
	Mandatory – This module needs to be completed and passed every 12 months.
	Recommended - all staff may undertake any of these modules and, in some cases, maybe required to do so at the request of individual managers.